The opinion in support of the decision being entered today was *not* written for publication and is *not* binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte BARRY ATKINS, DAVID CARROLL CHALLENER, FRANK NOVAK, JOSEPH GARY RUSNAK, KENNETH D. TIMMONS, and WILLIAM W. VETTER

Appeal 2006-2482
Application 09/651,548
Technology Center 2100

Decided: April 5, 2007

MAILED
APR 05 2007
U.S. PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS
AND INTERFERENCES

Before LANCE LEONARD BARRY, MAHSHID D. SAADAT, and JEAN R. HOMERE, *Administrative Patent Judges*.

BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

An Examiner rejected claims 1-24. The Appellants appeal therefrom under 35 U.S.C. § 134(a). We have jurisdiction under 35 U.S.C. § 6(b).

A. THE INVENTION

The invention at issue on appeal concerns "cryptography." (Specification 1.) Cryptography involves encrypting data to provide security for the data. Before transmitting a message from one party to another, for example, a mathematical function known as a "cryptographic algorithm" is used to encrypt the message. (*Id.*) The most common cryptographic algorithms are key-based, where special knowledge of variable information called a "key," is required to decrypt an encrypted message. (*Id.*)

The Appellants opine that centralization of encryption and decryption at a server can lead to a problem in key management. More specifically, a client system is assigned a key provided to the user of the system. Various keys for various client systems are used and managed by the server. If the key issued for a particular client system needs to be revoked, the user may maintain a copy of the revoked key and thereby gain unlawful access to encrypted data. (*Id.* at 8.)

The Appellants assert that their invention consolidates the encryption and decryption in a centralized location while avoiding the aforementioned

problem. (*Id.*) A further understanding of the invention can be had by reading the following claim.

> 1. A method for managing a user key used to sign a message for a data processing system, said method comprising:
>
> assigning a user key to a user and storing the user key in an encrypting data processing system utilized to encrypt messages;
>
> encrypting the messages with the user key;
>
> storing an associated key in the encrypting data processing system and encrypting the user key with the associated key to obtain an encrypted user key;
>
> said encrypting data processing system communicating at least one encrypted message together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system; and
>
> thereafter, preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system.

B. THE REJECTIONS

Claims 1-3, 6-11, 14-19, and 22-24 stand rejected under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 6,807,277 ("Doonan") and U.S. Patent No. 6,009,177 ("Sudia"). Claims 4, 12, and 20 stand rejected under

§ 103(a) as obvious over Doonan, Sudia, and U.S. Patent No. 6,732,101 ("Cook"). Claims 5, 13, and 21 stand rejected under § 103(a) as obvious over Doonan, Sudia, Cook, and U.S. Patent No. 4,888,800 ("Marshall").

II. ISSUE

Rather than reiterate the positions of parties *in toto*, we focus on an issue therebetween. The Examiner admits, "Doonan does not specifically disclose using a certificate authority (trusted third party) for key validation and determination of key revocation," (Answer 4-5.), and "Doonan does not specifically disclose a usage of encryption key pairs and to revoke an encryption key pair." (*Id.* at 11.) The Examiner asserts, however, "Sudia discloses preventing validation of the association of the user with messages by revoking the associated key at the encryption data processing system (see Sudia col. 22, lines 51-63, col. 23, lines 4-7: access revocation list to determinate whether certificate (attached key) is valid)[.]" (*Id.* at 5.) Appellants argue that "the conventional publication of the recipient's public key on a CRL as taught by *Doonan* and *Sudia* does not revoke the public key 'at' the encrypting data processing system. . . ." (Br. 7.) Therefore, the issue is whether the prior art would appear to have suggested require encrypting system to revoke a key stored therein.

In addressing the issue, the Board conducts a two-step analysis. First, we construe the independent claims at issue to determine their scope.

Second, we determine whether the construed claims would have been obvious.

III. CLAIM CONSTRUCTION

"Analysis begins with a key legal question — what is the invention claimed?" *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1567, 1 USPQ2d 1593, 1597 (Fed. Cir. 1987). In answering the question, "the PTO gives claims their 'broadest reasonable interpretation.'" *In re Bigio*, 381 F.3d 1320, 1324, 72 USPQ2d 1209, 1210-11 (Fed. Cir. 2004) (quoting *In re Hyatt*, 211 F.3d 1367, 1372, 54 USPQ2d 1664, 1668 (Fed. Cir. 2000)).

Here, independent claim 1 recites in pertinent part the following limitations:

> assigning a user key to a user and storing the user key in an encrypting data processing system utilized to encrypt messages;
>
> storing an associated key in the encrypting data processing system and encrypting the user key with the associated key to obtain an encrypted user key;
>
> thereafter, preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system.

Independent claims 9 and 17 recite similar limitations. Giving the independent claims the broadest, reasonable construction, the limitations require an encrypting system to revoke a key stored therein.

IV. OBVIOUSNESS DETERMINATION

"Having determined what subject matter is being claimed, the next inquiry is whether the subject matter would have been obvious." *Ex Parte Massingill*, No. 2003-0506, 2004 WL 1646421, at *3 (B.P.A.I 2004). "In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a *prima facie* case of obviousness." *In re Rijckaert*, 9 F.3d 1531, 1532, 28 USPQ2d 1955, 1956 (Fed. Cir. 1993) (citing *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992)). "'A *prima facie* case of obviousness is established when the teachings from the prior art itself would appear to have suggested the claimed subject matter to a person of ordinary skill in the art.'" *In re Bell*, 991 F.2d 781, 783, 26 USPQ2d 1529, 1531 (Fed. Cir. 1993) (quoting *In re Rinehart*, 531 F.2d 1048, 1051, 189 USPQ 143, 147 (CCPA 1976)).

Here, Sudia explains that "[a] user who desires to send an encrypted communication to another user must have an escrow certificate for his own device and an escrow certificate for the intended recipient's public encryption key, because the device of the [the reference's] invention will neither encrypt

nor decrypt if either is missing." (Col. 21, ll. 15-20.) "[B]ecause the sender's device will not encrypt and the recipient's device will not decrypt unless the recipient's public encryption key certificate is 'valid,'" (*id.* at ll. 28-30), the device must first "verify the properties of the recipient's public encryption key certificate or of the digital signatures thereon. . . ." (*Id.* at ll. 57-58.)

The first part of Sudia cited by the Examiner discloses that "[w]henever any user, entity or device 'verifies' a digitally signed 'certificate,'" (col. 22, ll. 51-52.), the former "checks any applicable 'certificate revocation list' ('CRL') . . . to determine whether the certifying authority or other issuer has distributed, propagated or otherwise made available a list of revoked certificates . . . and whether, based upon the issuer name and certificate number, the certificate has been revoked." (*Id.* at ll. 57-63.) We find no teaching or suggestion in this part of the reference, nor the other part cited by the Examiner, however, that an encrypting user, entity, or device revokes a certificate or an intended recipient's public encryption key. To the contrary, we agree with Appellants that "[s]uch revocation can be said to be made 'at' the certifying authority that publishes the CRL. . . ." (Br. 7.)

In the *Response to Argument* section of his Answer, the Examiner refers to Cook for evidence of "the capability to revoke an association key pair by deleting an association encryption key pair." (Answer 12.) "Where a reference is relied on to support a rejection, whether

or not in a 'minor capacity,' there would appear to be no excuse for not positively including the reference in the statement of rejection." *In re Hoch*, 428 F.2d 1341, 1342 n.3, 166 USPQ 406, 407 n.3 (CCPA 1970). Here, although the Examiner refers to Cook for the capability to revoke an association key, he fails to include the reference in the statement of the rejection of claims 1-3, 6-11, 14-19, and 22-24. Consequently, we cannot consider the teachings of the reference in this regard. Furthermore, the Examiner does not allege, let alone show, that the addition of Marshall cures the aforementioned deficiency of Doonan and Sudia.

V. CONCLUSION

Absent a teaching or suggestion that an encrypting system revokes a key stored therein, we are unpersuaded of a prima facie case of obviousness. Therefore, we reverse the rejections of claims 1, 9, and 17 and of claims 2-8, 10-16, and 18-24, which depend therefrom.

REVERSED

kis/gw

DILLON & YUDELL, LLP
8911 NORTH CAPITAL OF TEXAS HWY, SUITE 2100
AUSTIN, TX 78759